Mobile Forensics Development of Mobile Banking Application using Static Forensic

By Imam Riadi

Mobile Forensics Development of Mobile Banking Application using Static Forensic

Adam Prayogo Kuncoro
Department of Informatics
STMIK Amikom
Purwokerto, Indonesia

Imam Riadi
Department of Information Systems
Ahmad Dahlan University
Yogyakarta, Indonesia

Ahmad Luthfi
Department of Informatics
Islamic University of Indonesia
Yogyakarta, Indonesia

ABSTRACT

Modern society often conducts transactions through the banking system in many purposes. Suppose transfers between accounts or between banks, monthly subscription payments, and so forth. To facilitate such transactions, many banks provide a service to customers in the form of mobile banking applications. But the increasingly sophisticated technology used in providing the service, the greater the threat of cybercrime in the world around customers. By way of forensic analysis forensic data with the static method expected to obtain important information or data that can be used as digital evidence. Suppose the access log, transaction records, customer profiles, and so on. Because the important information that can be misused as a security loophole to carry out illegal access. This study focused on the analysis of the log data mobile banking application, expected results reached 80%. After testing and analysis of the mobile banking application, there is no important information that can be used for unauthorized access. And the security level applied modern enough to secure from unauthorized access action.

Keywords

Mobile Banking, Mobile Forensics, Log, Security

1. INTRODUCTION

Nowadays people do banking transactions through for various purposes. For example, money transfers, payment of a monthly subscription, and others. To facilitate the transaction, any banks providing services to the customers. Providing services such as Mobile Banking application.

Mobile banking application is software that can be embedded into a smartphone. Mobile banking can be defined as the ability to perform banking transactions through a mobile equipment, or more broadly to carry out financial transactions through mobile terminal [1].

Mobile banking facility to assist and facilitate community purposes in conducting needs relating to banking transactions. Mobile banking has the ability to perform banking activities virtually any time (no time limit) and anywhere (without limitation location) [2].

The increasing use of mobile banking application services currently subjects to risk and danger from the perpetrators of cybercrime which could result in material losses. One of the crimes that may occur in the use of mobile banking is duplicate or cloned authorizing access mobile banking. The banking system does not know whether the transactions made on the mobile banking facility is actually derived from the original customer account owner or not.

Researchers aim to find digital evidence and critical information as a potential crime or vulnerability of the mobile banking services. Some examples of important information related to mobile banking services that the customer account, log history, transaction history and customer profile. The important information is the vulnerability of digital crime.

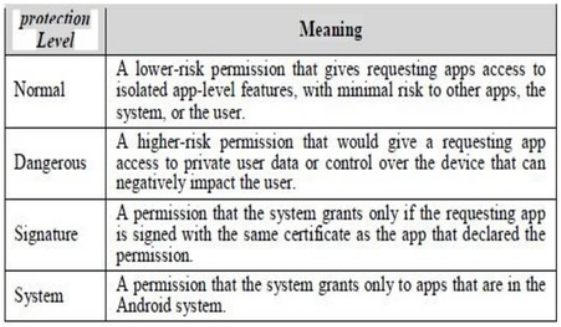
Sphere of interest which will be conducted by researchers are digging potential as digital evidence contained in the application of mobile banking as an effort to help complete the information on the activity of mobile forensic and analyze the security level applied.

2. CURRENT RESEARCH

Current development shows that there is an increasing number of mobile users for internet banking transactions in the midst of modern society. Mobile banking technology allows people to conduct transactions anytime and anywhere. Therefore banks currently offer a variety of mobile transaction services to facilitate customers. And the provision of mobile electronic services like that only costs a relatively more expensive when compared to the cost of placing an ATM machine (Automated Teller Machine) along with maintenance costs [3].

People who use mobile banking facility has a level of sensitivity of the personal information that they give in financial transactions. The researchers analyzed the use of mobile banking application on the rights of access provided as a security mechanism in the application. Permission system permissions are embedded in a mobile banking application can cause serious effects if the security level is known by others and used in accordance owner's actual access [4]. It is illustrated in Table 1.

Table 1 : Analysis of the level security [4].



protection Level	Meaning
Normal	A lower-risk permission that gives requesting apps access to isolated app-level features, with minimal risk to other apps, the system, or the user.
Dangerous	A higher-risk permission that would give a requesting app access to private user data or control over the device that can negatively impact the user.
Signature	A permission that the system grants only if the requesting app is signed with the same certificate as the app that declared the permission.
System	A permission that the system grants only to apps that are in the Android system.

Researchers looked at hacking actions against global banking account (in the world) has caused inestimable losses. That is because there are many weaknesses in the banking system, in particular the researchers analyzed the security system on the mobile banking application. Analysis conducted aimed at identifying and classifying embedding security at the mobile banking system. The results found in the study was the use of encrypted security level, there is a system of authentication and authorization are layered, and there is a network layer security system [5].

Mobile banking application is attractive because it is convenient to be used, although there are still security gaps. Researchers analyzed the security system on a GSM network that is used to operate a mobile banking application is meant to connect with the banking server [6]. Security Protocol-Based Mobile Banking SMS with Formal Verification, is a proposal on a new protocol to be embedded in the security of mobile banking applications. The system will be implanted at the level of authentication and payment is expected to provide security in SMS communication between the customer and the bank system through a mobile banking application [7].

3. BASIC THEORY

A. Mobile Banking

Mobile banking is banking service that applying information technology. Mobile banking or so-called m-banking is a banking service provided by the bank to support the smoothness and ease of banking activities. The effectiveness and efficiency of customers to conduct mobile banking transactions will not run if it is not supported by the mobile phone and internet networks.

Although both of use a mobile phone as a means, mobile banking has newer technologies for using an application that must be downloaded and installedon a smartphone, compared to SMS-banking wich is only by means of Short Message Service (SMS) [8]. Figure 1 is security system of mobile network protocols and server security bank [8].

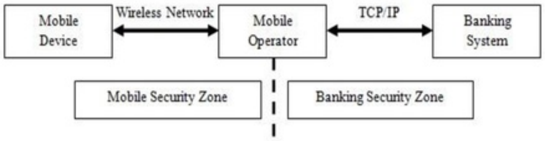


Figure 1 : Illustration of security on mobile networks and the bank server

B. Mobile Forensic

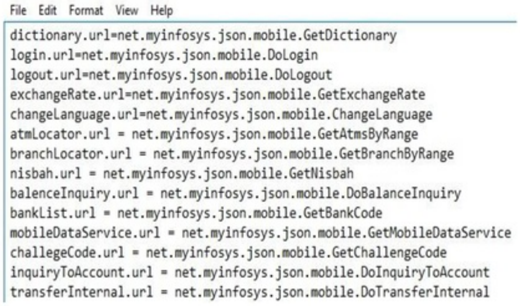
Digital Forensic to review important information contained in the digital electronic devices for specific purposes, such information can be obtained and used as digital evidence legally before the law. There are also audio forensic, image forensic, and others.

While on mobile forensic science is one of the main parts of the digital forensic science. Mobile forensic is the science that related to electronic devices that can be taken anywhere and it easy to move (mobile). For example, mobile phones, smartphones, GPS devices, etc. [9].

The information wich can be analyzed in the science of mobile forensic usually SMS history, call log, contact telephone number on the cell phones and the crucial information that are found in the smartphone apps wich canbe used as digital evidence, and various other information related to digital evidence [10].

C. Log

Basically, the process of acquisition and investigation of solving cases using digital evidence includes in the digital forensic science. In the digital forensic science, there are two methods regarding acquisition techniques, namely live forensic and forensic static. The example of log data acquisition related to digital evidence from mobile device shown in Figure 2.



```
dictionary.url=net.myinfosys.json.mobile.GetDictionary
login.url=net.myinfosys.json.mobile.DoLogin
logout.url=net.myinfosys.json.mobile.DoLogout
exchangeRate.url=net.myinfosys.json.mobile.GetExchangeRate
changeLanguage.url=net.myinfosys.json.mobile.ChangeLanguage
atmLocator.url = net.myinfosys.json.mobile.GetAtmsByRange
branchLocator.url = net.myinfosys.json.mobile.GetBranchByRange
nisbah.url = net.myinfosys.json.mobile.GetNisbah
balenceInquiry.url = net.myinfosys.json.mobile.DoBalanceInquiry
bankList.url = net.myinfosys.json.mobile.GetBankCode
mobileDataService.url = net.myinfosys.json.mobile.GetMobileDataService
challegeCode.url = net.myinfosys.json.mobile.GetChallengeCode
inquiryToAccount.url = net.myinfosys.json.mobile.DoInquiryToAccount
transferInternal.url = net.myinfosys.json.mobile.DoTransferInternal
```

Figure 2 : Example of log data acquisition

The difference is that the live forensic analysis is performed live or in person when the device is active (in a position connected to the network), while static forensic analysis is a technique used in off-line evidence, when it is not connected to the network and investigators can immediately handle the evidence to be acquired.

For example, the forensic analysis uses static techniques on a hard disk wich can be directly analyzed. Other example is when analyzing the mobile device (mobile phone or smartphone) that can be done without connecting to the wireless network.

The static forensic analysis is done through the static, data is preserved (stored through the cloning process beforehand) on a permanent storage media. Not all the data need to understand the circumstances (investigation) of the system wich are examined [11].

4. RESEARCH METHOD

To perform mobile forensic investigation by a forensic static method on a mobile banking applications need to conduct acquisition and analysis with the following steps. Figure 3 is a static forensic acquisition process.

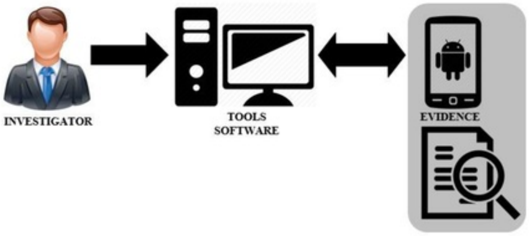


Figure 3 : Static forensic illustration

Static forensic process is used conduct detailed analysis stage and careful review of the application system without being connected to the banking system through the network (offline). For example, in the form of relevant customer profile data, transaction logs, account number of the account owner and the account associated with the data of past transactions and other important data.

The investigation process is the last phase that preceded the examination and analysis of digital evidence. By using the tools that have been prepared, we did a systematic and detailed analysis.The analysis process is done manually to find the data of suspected illegal transaction records. As well as manual analysis steps carried out for the required accuracy of data search.

Our execution data on potential digital evidence directly fixed on the smartphone device that is used as a medium of mobile banking transactions. The next process is the classification of data wich have important information related to digital evidence or vulnerability, and data are not included in the digital evidence.

Handling process design and analysis of evidence are illustrated in Figure 4. This process is adopting the research that was done on a smartphone using mobile forensic analysis [12].

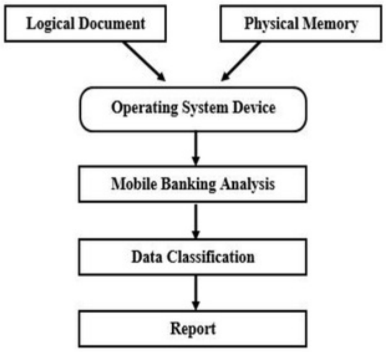


Figure 4 : Research analysis design

5. RESULT

A. Handling Process

Today many people have a mobile device that every day is used for official and personal purposes. One of them is used as supporting transactional activity. It is in the form of Android-based smartphones. In addition, this device is handled as a potential source of digital evidence.

Simulation of cases in this study is a fraud or embezzlement access illegally outside the authorized account owner's knowledge. The media of acquisition and analysis in this study is a mobile device such as smartphones based on Android. Fraud action is taken in order to break into the mobile banking app access.

This study aims to analyze the potential of digital evidence in the smartphone. The digital evidence can be a data that describes the illegal actions access records or other supporting data. In addition, this study also analyzes the mobile banking applications to find vulnerabilities that can be exploited for illegal actions.

This stage contains the detection or identification device as potential digital evidence. Any evidence related to the handling of cases should be done immediately; it is due to the effectiveness and efficiency of handling follow the disclosure of evidence which must be appropriate and accurate.

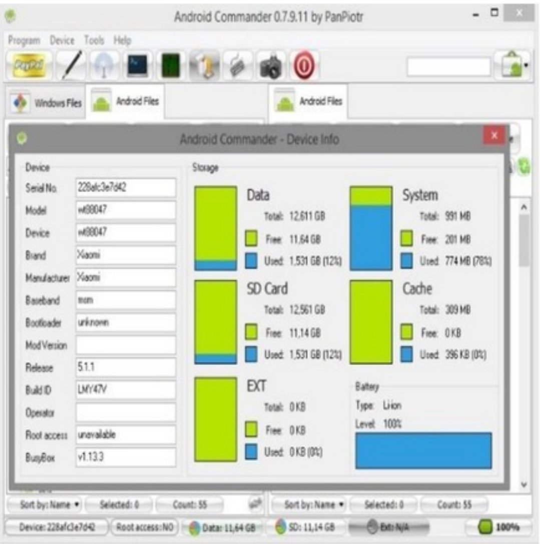
B. Acquisition Process

The acquisition process aims to collect data on the installed smartphone mobile banking application. At this stage logical data retrieval is done. This is done by using the Android software Commander and FTK Imager to process the imaging data. Using the Android Commander application.

This process separates the customer's mobile device, the device that will be handled with devices that are not potentially as digital evidence. The process of recording must be made clearly, including the name, type, serial number or other identification found on the evidence. Additionally, it is necessary to conduct detailed recording of the officer who made the handling of evidence.

At the time of acquisition, the smartphone should be on standby and mobile banking applications are not in the online state. Stages of the acquisition process using USB as a connection between a smartphone device with a computer. To avoid contamination and maintain the integrity of the data during the withdrawal process will require security using software USB Write Blocker.

Stages of data acquisition are done using Android software Commander can be seen in Figure 5.



Device

Serial No. 228alc3e7d42
Model wt88047
Device wt88047
Brand Xiaomi
Manufacturer Xiaomi
Baseband msm
Bootloader unknown
Mod Version
Release 5.1.1
Build ID LMY47V
Operator
Root access unavailable
BusyBox v1.13.3

Storage

Data
Total: 12,611 GB
Free: 11,64 GB
Used: 1,531 GB (12%)

System
Total: 991 MB
Free: 201 MB
Used: 774 MB (78%)

SD Card
Total: 12,561 GB
Free: 11,14 GB
Used: 1,531 GB (12%)

Cache
Total: 309 MB
Free: 0 KB
Used: 396 KB (0%)

EXT
Total: 0 KB
Free: 0 KB
Used: 0 KB (0%)

Battery
Type: Li-ion
Level: 100%

Device: 228afc3e7d42 | Root access: NO | Data: 11,64 GB | SD: 11,14 GB | Ext: N/A | 100%

Figure 5 : Data acquisition process

The next stage is the process of digital imaging. The cloning process performed imaging data from smartphone devices. To ensure the authenticity of the data that has been acquired,recording a hash value on the data imaging results needs to be conducted. In addition there is some important information that should be recorded, such as the time of acquisition, the hash value, and data size imaging results. This is done because the hash value information clones will be verified with the hash value in the data analysis results.

The result of the imaging process data using software FTK Imager is shown in Table 2.

Table 2 : Recording information on the results of digital imaging

Name	AndroidDevice.ad1
Data Source	*Logical*
Time of Acquisition	Sun Sep 04 00:34:53 2016
	Sun Sep 04 00:50:27 2016
Hash	MD5 : 7d8954fb347142635fe410972dac0dee
	SHA1 :

	d5827b4c27f87be799ec4734fc8e6145 672c0167
Application	AccessData® FTK® Imager 3.1.0.1514

Than the results of the data acquisition process is performed in the form of safe handling and security.

C. The Process of Investigation and Analysis

a) Analysis of Process Flow

Explanation of process flow analysis conveyed about the mobile banking points - points that are generally common and used by bank customers. For examples steps to log in, checking balances, transaction banking, and log out. The step of workflow mobile banking application is illustrated in Figure 6.

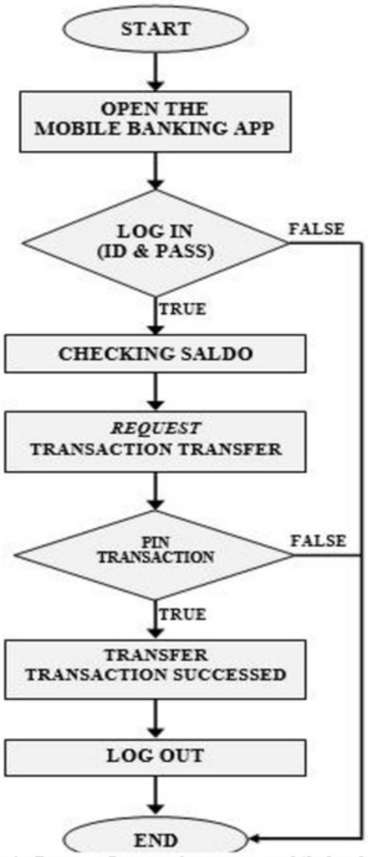

START
OPEN THE MOBILE BANKING APP
LOG IN (ID & PASS)
FALSE
TRUE
CHECKING SALDO
REQUEST TRANSACTION TRANSFER
PIN TRANSACTION
FALSE
TRUE
TRANSFER TRANSACTION SUCCESSED
LOG OUT
END

Figure 6 : Process flow performance mobile banking application

There are two (2) keys to access attestation of the process flow of mobile banking applications. The first is the validation of access password key when logging in the application, which serves as an access authentication approval to enter into the application system. The second access key is PIN which is used to validated permissions for banking transactions.

b) Data Analyze

At the stage of the analysis performed on data from imaging observations using FTK Imager software. Observations aim to find components that are potential as digital evidence related to mobile banking applications. The results of observation are summarized in Table 3.

Table 3 : Data result of observation

Folder	File
acct	uid (folder) $I30, cgroup.clone_children, cgroup.procs, cgroup.sane_behavior, cpuacct.stat, cpuacct.usage, cpuacct.usage_percpu, notify_on_release, release_agen,tasks
bin	adb_keys
mnt - shell - emulated	.dlprovider (folder), Android (folder), jeejen (folder), libs (folder), miad (folder), MIUI (folder), Movies (folder), Pictures (folder), system (folder) $I30, .profig.os, .volume
Proc	327 (folder), asound (folder), bus (folder), driver (folder), fs (folder), irq (folder), scsi (folder), sys (folder), sysvipc (folder), touchscreen (folder), tty (folder) $I30, buddyinfo, cgroups, consoles, cpuinfo, crypto, devices, diskstats, execdomains, fb, filesystems, ft5x0x-debug
res - images - charger	$I30, battery_fail.png, battery_scale_0.png, battery_scale_1.png, battery_scale_2.png, battery_scale_3.png, battery_scale_4.png, battery_scale_5.png
Storage	sdcard 1 (folder)
sys	bus (folder), devices (folder), fs (folder)
system	app (folder), bin (folder), etc (folder), fonts (folder), framework (folder), lib (folder), media (folder), priv-app (folder), tts (folder), usr (folder), vendor (folder), xbin (folder) $I30, built.prop, built.prop.bakforspec
(main directori)	$I30, default.prop, file_contexts, property_contexts, seapp_contexts, selinux_version, sepolicy, service_contexts, ueventd.qcom.rc, ueventd.rc, unlock_key, verity_key

The results of the observations that had been conducted on the data which is shown in Table 3 did not reveal any potential digital evidence related variables, content and folders in it. Based on observations described in Table 3, it can be concluded that mobile banking applications along with a directory of storage on a smartphone are not found the necessary data relating to the account of customers, of identity along with the access key, the log records application access, record banking transactions records as well as the third transactions party services, and there are no other important data that can be used as security holes in the mobile banking applications.

c) Analysis of Security Systems
At this stage, an analysis of the mobile banking application security system to determine the level of security with the observations is described in detail in Table 4.

Table 4 : Observation of security level

Security System	Security Level	Information
Telephone numbers SIM Card Authentication	Medium Risk	There is no detection process to authenticate the SIM Card phone number used on smartphones as a legitimate customer identification corresponding banking data at the beginning of the registration of activation of mobile banking services
Authentication access application (ID and password)	Low Risk	Customers are required to update or change the password within 30 days for any use of the access password
Data stored / transaction log	Low Risk	There are no transaction history record data, access logs, the client's identity, and other important data related to banking authorized account
Authentication access banking transactions and additional third-party services PIN 6 (six) digits	Low Risk	Security systems such as access PIN 6 (six) digit must be differentiated access key applications. And when transactions must fill two (2) random PIN code corresponding application command

There are weaknesses in the authentication phase to ensure that the SIM card inside the smartphone there is a SIM card with a mobile phone number of the user's identity or the customer is entitled to access to the application.

Authentication security in the form of SIM Card access scanning is used as security for the first phase before continuing on the stage login access. The application will automatically shut down or force to close when the system has ensured inside the smartphone there is no SIM card that includes a mobile phone number is registered on the bank system.

6. CONCLUSION

Researchers have conducted a series of studies and analysis of mobile banking applications, it can be concluded, the basic command system in the process flow of mobile banking applications practice not to store important data belonging to customers as a legal and legitimate access. The conclusions of this study have made it clear that in this smartphone device was not found important data that can be used as digital evidence of potential or vulnerabilities.

The command script application works only make requests access to the services provided by banks through the application. Mobile banking applications and functions only as an intermediary access without storage of information that have been accessed by the customer. Based on the study, mobile banking applications had some stages of security system in the form of identity access authentication and password or PIN that had to be entered into the system. The use of PIN lock transaction can be distinguished by a password / PIN entry applications. And a working system using a password / PIN entry replacement should be done periodically by the application system.

This study focused on the analysis of the log data mobile banking application, expected results reached 80%. After testing and analysis of the mobile banking application, there is no important information that can be used for unauthorized access. And the security level applied modern enough to secure from unauthorized access action.

7. FUTURE WORKS

The suggestion is a medium to convey a shortage of researchers in the process and complete the study, therefore the researchers expect a lot of suggestions from the readers and others researchers on related fields in this study. Since the limited tools or applications which can support the research on the mobile forensics investigators, the researchers need additional information to enlarge the knowledge about it from the other studies. The suggestion for the next research is using a live forensic method or perform physical acquisition of the mobile device.

8. REFERENCES

[1] I.Advances and C. Technology, "Discovering Authentication Credentials in Volatile Memory of Android Mobile Devices," no. April 2013, 2016.

[2] A. Hussain, H. I. Abubakar, and N. B. Hashim, "Evaluating mobile banking application: Usability dimensions and measurements," *Conf. Proc. - 6th Int. Conf. Inf. Technol. Multimed. UNITEN Cultiv. Creat. Enabling Technol. Through Internet Things, ICIMU 2014*, no. 1, pp. 136–140, 2015.

[3] M. Purwanegara, A. Apriningsih, and F. Andika, "Snapshot on Indonesia Regulation in Mobile Internet Banking Users Attitudes," *Procedia -Social Behav. Sci.*, vol. 115, no. Iicies 2013, pp. 147–155, 2014.

[4] T. Cho, Y. Kim, and S. Han, "Potential Vulnerability Analysis of Mobile Banking Applications," no. 2012, pp. 1114–1115, 2013.

[5] L. Nosrati, "Security assessment of Mobile- Banking," pp. 1--5, 2015.

[6] C. Narendiran, S. A. Rabara, and N. Rajendran, "Public key infrastructure for mobile banking security," *2009 Glob. Mob. Congr.*, pp. 1–6, 2009.

[7] S. Bojjagani and V. N. Sastry, "SSMBP: A secure SMS-based mobile banking protocol with formal verification," *2015 IEEE 11th Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2015*, pp. 252–259, 2015.

[8] S. Hadi and U. I. Indonesia, "Faktor-Faktor Yang Mempengaruhi Penggunaan," pp. 55–67.

[9] M. Epifani, S. European, and D. Forensics, “Open Source Tools for Mobile Forensics,” no. October, 2013.

[10] Y. Wang and Y. Alshboul, “Mobile security testing approaches and challenges,” *2015 First Conf. Mob. Secur. Serv.*, pp. 1–5, 2015.

[11] Mrdovic, A. Huseinovic, and E. Zajko, “Combining static and live digital forensic analysis in virtual environment,” *IEEE Int. Symp. Information, Commun. Autom. Technol.*, pp. 1–6, 2009.

[12] Z. Qian, D. Luo, and S. Wu, “Analysis and design of a mobile forensic software system based on AT commands,” *2008 IEEE Int. Symp. Knowl. Acquis. Model. Work. Proceedings, KAM 2008*, no. 60704042, pp. 597–600, 2008.

Mobile Forensics Development of Mobile Banking Application using Static Forensic

ORIGINALITY REPORT

4%

SIMILARITY INDEX

PRIMARY SOURCES

1	Advances in Intelligent Systems and Computing, 2016. Crossref	35 words —	1%
2	Mohammadi, Hossein. "A study of mobile banking loyalty in Iran", Computers in Human Behavior, 2015. Crossref	19 words —	1%
3	eprints.binadarma.ac.id Internet	17 words —	< 1%
4	warse.org Internet	15 words —	< 1%
5	Sasa Mrdovic. "Forensic analysis of encrypted volumes using hibernation file", 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers, 11/2011 Crossref	14 words —	< 1%
6	dblp.dagstuhl.de Internet	14 words —	< 1%
7	Zulfadhilah, Muhammad, Yudi Prayudi, and Imam Riadi. "Cyber Profiling Using Log Analysis And K-Means Clustering", International Journal of Advanced Computer Science and Applications, 2016. Crossref	13 words —	< 1%
8	"VCR : App-Agnostic Recovery of Photographic Evidence from Android Device Memory Images", Proceedings of the 22nd ACM SIGSAC Conference on Computer	12 words —	< 1%

and Communications Security - CCS 15, 2015.
Crossref

9 Kim, Hyang-mi, Han-na Lee, and Sangkyung Kim. "Grouping Resource Allocation Scheme for D2D Communications", The Journal of Korean Institute of Communications and Information Sciences, 2015.
Crossref
9 words — < 1%

10 "Localization to Bidirectional Languages for a Visual Programming Environment on Smartphones", International Journal of Computer Science Issues, 2017
Crossref
9 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		